



# UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/993,495	11/27/2001	Doug Rollins	M4065.0486/P486	8165

24998 7590 10/17/2005

DICKSTEIN SHAPIRO MORIN & OSHINSKY LLP  
2101 L Street, NW  
Washington, DC 20037

EXAMINER

GELAGAY, SHEWAYE

ART UNIT PAPER NUMBER

2137

DATE MAILED: 10/17/2005

Please find below and/or attached an Office communication concerning this application or proceeding.



## **DETAILED ACTION**

1. This office action is in response to Applicant's amendment filed on August 1, 2005. Claims 1, 5-6, 8, 15-17 and 20 have been amended. Claims 1-26 are pending.

### ***Drawings***

2. In view of the amendment filed August 1, 2005, the Examiner withdraws the objection to the drawings.

### ***Claim Rejections - 35 USC § 112***

3. In view of the amendment filed August 1, 2005, the Examiner withdraws the rejection of claim 5 under 35 U.S.C. 112.

### **Response to Arguments**

4. Applicant's arguments with respect to claims 1-26 have been considered but are moot in view of the new ground(s) of rejection.

### ***Claim Rejections - 35 USC § 103***

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: 2133

6. Claims 1-3, 6-10, 13-17, 20-23 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Roche et al. (hereinafter Roche) EP-1050991 in view of Ahvenainen United States Letters Patent Number 6,199,161.

As per claim 1:

Roche teaches a method of updating an encryption key in a wireless network, said method comprising:

a communication device containing an encryption key from a wireless station of said network; (Col. 5, lines 43-58 and Col. 6, line 6)

connecting said removed communications device to a wired portion of said network which contains an encryption key generator; (Col. 6, lines 20-52; Col. 10, lines 43-45)

replacing an existing encryption key in said communications device with a new encryption key from said generator using a communication over said wired portion of said network; (Col. 6, lines 46-52) and

Roche does not explicitly disclose physically separating and connecting a communication device and a wired and wireless network.

Ahvenainen in analogous art, however, discloses a mobile communication system with SIM card that contain identifiers and keys and which may be attached to the mobile station detachably. The card can be physically removed from mobile equipment. The card offers services to the mobile station like inputting and changing PIN or key. (Col. 2, lines 7-12 and lines 24-46; Col. 7, lines 30-35; Col. 10, lines 11-12)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Roche to include physically separating and connecting a communication device and a wired and wireless network. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Ahvenainen (Col. 8, lines 2-5) in order to a centralized place, a key generator, in which keys are programmed in the center and on the cards.

As per claims 2 and 22:

Roche and Ahvenainen teach all the subject matter as discussed above. In addition, Roche further discloses a method wherein said new encryption key is generated at user-defined intervals. (Col. 6, lines 46-47 and lines 53-55)

As per claims 3 and 23:

Roche and Ahvenainen teach all the subject matter as discussed above. In addition, Roche further discloses a method wherein said new encryption key is generated on user-specified days. (Col. 6, lines 46-47 and lines 53-55)

As per claims 6 and 16:

The combination of Roche and Ahvenainen teach a method of changing encryption key using a plug-in card in a wireless network by connecting and separating with the wired network. In addition, Ahvenainen further discloses a wireless station wherein said network communications device is adapted to be physically connected to a wired network by being insertable into card tray physically connected to said wired network. (Col. 2, lines 7-12 and lines 24-46; Col. 7, lines 30-35; Col. 10, lines 11-12)

As per claim 7:

Roche and Ahvenainen teach all the subject matter as discussed above. In addition, Roche further discloses a method wherein a plurality of network communications devices can be inserted into said card tray simultaneously. (Col. 9, lines 51-55)

As per claims 8 and 15:

Roche teaches a wireless network comprising:

a wired station connected to a wired network, (Figure 1) said wired station comprising:

an encryption key generator for generating an encryption key; (Col. 6, lines 20-52; Col. 10, lines 43-45) and

a wired network communications device for transmitting said encryption key over said wired network; (Col. 6, lines 20-52)

an encryption key transmitted over said wired network by said wired network communications device. (Col. 6, lines 46-52)

Roche does not explicitly disclose a wireless network communications device being physically disconnectable from said wireless station and physically connectable to said wired network to receive and store as a new encryption key.

Ahvenainen in analogous art, however, discloses a mobile communication system with SIM card that contain identifiers and keys and which may be attached to the mobile station detachably. The card can be physically removed from mobile

Art Unit: 2133

equipment. The card offers services to the mobile station like inputting and changing PIN or key. (Col. 2, lines 7-12 and lines 24-46; Col. 7, lines 30-35; Col. 10, lines 11-12)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Roche to include a wireless network communications device being physically disconnectable from said wireless station and physically connectable to said wired network to receive and store as a new encryption key. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Ahvenainen (Col. 8, lines 2-5) in order to a centralized place, a key generator, in which keys are programmed in the center and on the cards.

As per claims 9 and 21:

The combination of Roche and Ahvenainen teach a method of changing encryption key using a plug-in card in a wireless network by connecting and separating with the wired network. In addition, Roche further discloses a new encryption key is a randomly generated encryption key. (Col. 10, lines 49-52)

As per claim 10:

The combination of Roche and Ahvenainen teach a method of changing encryption key using a plug-in card in a wireless network by connecting and separating with the wired network. In addition, Roche further discloses a new encryption key is generated by said generator and transmitted by said wired network communications device at user-defined intervals. (Col. 6, lines 46-47 and lines 53-55)

As per claim 13:

The combination of Roche and Ahvenainen teach a method of changing encryption key using a plug-in card in a wireless network by connecting and separating with the wired network. In addition, Ahvenainen further discloses a plurality of access points. (Page 1, paragraph 8)

As per claims 14 and 26:

The combination of Roche and Ahvenainen teach a method of changing encryption key using a plug-in card in a wireless network by connecting and separating with the wired network. In addition, Roche further discloses a card tray connected to said wired network, said wireless network communications device being connected to said wired network by insertion of said wireless network communications device into said card tray. (Col. 9, lines 51-55)

As per claim 17:

Roche discloses a device comprising: a storage area said network card which stores an updateable encryption key for use in conducting encrypted wireless network communications, (Col. 10, lines 47-49) said encryption key being updateable when said card is connected to a wired network card interface which supplies a new encryption key. (Col. 6, lines 20-52; Col. 10, lines 43-45)

Roche does not explicitly disclose a removable wireless communications network card adapted to be physically connected to a wireless station card interface.

Ahvenainen in analogous art, however, discloses a mobile communication system with SIM card that contain identifiers and keys and which may be attached to the mobile station detachably. The card can be physically removed from mobile



Art Unit: 2133

equipment. The card offers services to the mobile station like inputting and changing PIN or key. (Col. 2, lines 7-12 and lines 24-46; Col. 7, lines 30-35; Col. 10, lines 11-12)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Roche to include a removable wireless communications network card adapted to be physically connected to a wireless station card interface. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Ahvenainen (Col. 8, lines 2-5) in order to a centralized place, a key generator, in which keys are programmed in the center and on the cards.

As per claim 20:

Roche teaches an encryption key programming system comprising:

an encryption key generator connected to a wired network; (Col. 6, lines 20-52; Col. 10, lines 43-45)

a programming device connected to said wired network for receiving over a wire connection an encryption key from said generator, said programming device being adapted to storing said received encryption key (Col. 10, lines 47-49)

Roche does not explicitly disclose adapted to physically receive a wireless network communication device.

Ahvenainen in analogous art, however, discloses a mobile communication system with SIM card that contain identifiers and keys and which may be attached to the mobile station detachably. The card can be physically removed from mobile

Art Unit: 2133

equipment. The card offers services to the mobile station like inputting and changing PIN or key. (Col. 2, lines 7-12 and lines 24-46; Col. 7, lines 30-35; Col. 10, lines 11-12)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Roche to include a removable wireless communications network card adapted to be physically connected to a wireless station card interface. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Ahvenainen (Col. 8, lines 2-5) in order to a centralized place, a key generator, in which keys are programmed in the center and on the cards.

7. Claims 4-5, 11-12, 24-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Roche et al. (hereinafter Roche) EP-1050991 in view of Ahvenainen United States Letters Patent Number 6,199,161 and further in view of Triege United States Letter Patent Number 6,226,750.

As per claims 4, 11 and 24:

Roche and Ahvenainen teach all the subject matter as discussed above. Both references do not explicitly disclose a method wherein said key generator generates a first new encryption key; compares said new encryption key to the previous k encryption keys used in said network; and generates a second new encryption key if said first new encryption key matches any of said k previously used encryption keys.

Trieger in analogous art, however, discloses a method wherein said key generator generates a first new encryption key; (Col. 11, lines 30-32) compares said new encryption key to the previous k encryption keys used in said network; (Col. 11, lines 39-41) and generates a second new encryption key if said first new encryption key matches any of said k previously used encryption keys. (Col. 11, lines 38-43)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Roche and Ahvenainen to include wherein said key generator generates a first new encryption key; compares said new encryption key to the previous k encryption keys used in said network; and generates a second new encryption key if said first new encryption key matches any of said k previously used encryption keys. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Trieger (Col. 11, lines 38-39) in order to ensure the previous key is not reused.

As per claims 5, 12 and 25:

Roche, Ahvenainen and Trieger teach all the subject matter as discussed above. In addition, Trieger further discloses a method wherein k is a user-defined number of previously used encryption keys. (Col. 11, lines 38-43)

8. Claims 18-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Roche et al. (hereinafter Roche) EP-1050991 in view of Ahvenainen United States

Letters Patent Number 6,199,161 and further in view of Serceki et al. (hereinafter Serceki) United States United States Publication Number 2003/0078072.

As per claim 18:

The combination of Roche and Ahvenainen teach a method of changing encryption key using a plug-in card in a wireless network by connecting and separating with the wired network. Both references do not explicitly disclose card interface for providing a new encryption key is a PCMCIA card interface.

Serceki in analogous art, however, discloses card interface for providing a new encryption key is a PCMCIA card interface. (Page 3, paragraphs 31-32)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Roche and Ahvenainen to include card interface for providing a new encryption key is a PCMCIA card interface. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Serceki (Page 3, Paragraph 31) in order to use a special connector that adheres to a common computer interface specification.

As per claim 19:

The combination of Roche, Ahvenainen and Serceki teach a method of changing encryption key using a plug-in card in a wireless network by connecting and separating with the wired network and PCMCIA card interface. In addition, Serceki further discloses said PCMCIA card interface is provided at a PCMCIA card tray. (Page 3, Paragraph 31)

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO 892.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

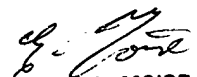
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on 571-272-3819. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2133

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shewaye Gelagay  
10/07/05



EMMANUEL L. MOISE  
SUPERVISORY PATENT EXAMINER